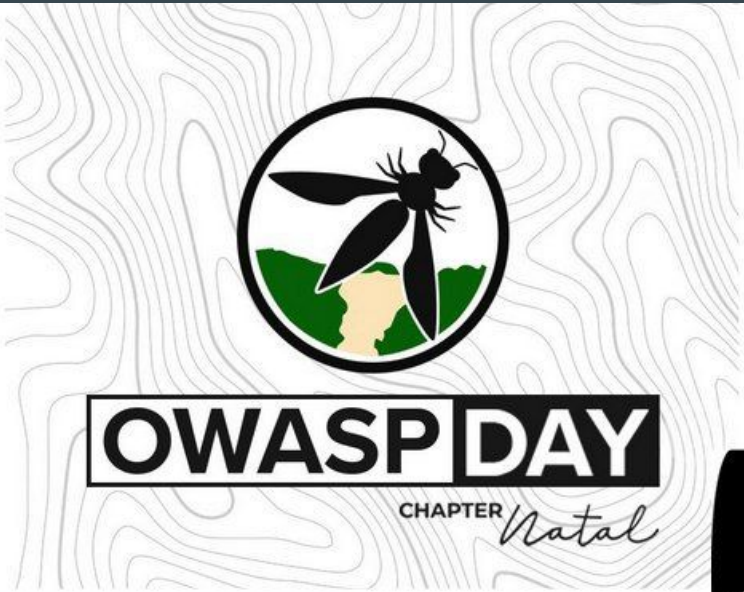
APOIO:


elastic


OWASP DAY
CHAPTER Natal


DARKWAVES


Qualitek


NERD & HACKER
IMAGINÁRIO NERD


Y4K


TEMPEST
security intelligence


LIVRO 1
BE MY GUEST
UMA ABORDAGEM PRÁTICA AO HACKING
Gustavo Abu

Kit de inteligência: OSINT Docker

...

Inteligência

HUMINT: Inteligência humana, informante, Vítima, Suspeito.

GEOINT: Satélite, drone, inteligência geográfica.

MASINT: Medição de assinatura de eventos, checkpoints que possam indicar um próximo ataque ou ato.

OSINT: Inteligência que estudam fontes abertas e acessíveis, a fim de obter o máximo de informações de seu alvo/inimigo.

SIGINT: Inteligência que estuda sinais, subdividia em: Comint (comunicações) e Elint (Inteligência eletrônica).

Open Source Intelligence (OSINT)

OSINT é definida como a análise baseada na “obtenção legal de documentos oficiais sem restrição de segurança, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia, da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança.” (CEPIK, 2003, p. 32)

PTES

INTERAÇÕES INICIAIS

Primeiro contato de primeira vista de seu alvo, onde ja pode ser levado considerações de funcionamento e afins

COLETA DE INFORMAÇÕES

Onde é realizado uma aprofundadda pesquisa de informações em geral tanto de seu funcionamento quato as suas versões, suas formas de desenvolvimento, e afins

MODELAGEM DE AMEAÇAS

Etapa na qual usará informações obtidas nos níveis anteriores para identificação de vulnerabilidades e fazer seu levantamento

ANÁLISE DE VULNERABILIDADES

Usando a informação do processo anterior são escolhidas as formas de ataques mais viáveis onde.

EXPLORAÇÃO

Enfim a realização do ataque afim de atingir o máximo em todas as vulnerabilidades encontradas.

PÓS-EXPLORAÇÃO

Onde será documentado todos os dados adquiridos através do pentest para que nada do ataque da fase anterior, se perca.

RELATÓRIO

Onde serão usadas todas as informações de todos os processos anteriores, expondo riscos e impactos.

Vault
CYBER SECURITY

vaultsecurity/osint

- Operative-framework: **operative framework is a OSINT investigation framework**
- D4N155: **Intelligent and dynamic wordlist using OSINT**
- Sherlock: **Find usernames across social networks**
- PhoneInfoga: **Advanced information gathering & OSINT tool for phone numbers**
- Karma: **Find leaked emails with your passwords**
- Recon-ng: **Recon-ng is a full-featured Web Reconnaissance framework written in Python**
- SE Toolkit: **The Social-Engineer Toolkit**
- OpenVas: **Open Vulnerability Assessment Scanner**

OWASP D4N155

bash main

ou

bash main -w scannme.nmap.org

bash main -t lista-de-urls.txt

```
jul10l1r4@ap:~/workspace/D4N155$ bash main -h

                    /\ o
              o    /_ /~/
               \     /\/
                \   /
                 \ /
              .{{}}}}}}.
            {{{{{}}}}}}.
           {{{{    {}{{}}}}
          }}}}} _    _ {{{{{
          }}}}  a   a  }}}&
         {{{{{    ^    {{{&
        }}}}}}\  .=.  /}}&&&
        {{{{{{{;.___.;}}&&&&
         '{{{{{{)   (}}|//&
          '''''':   :''''''

      [ At Segmentation Fault ]


   D4N155: Tool for smart audit security

   Usage: bash main <option> <value>
   All options are optionals
```

```
♥ sherlock ❯
```

PhoneInfoga

```
usage: phoneinfoga.py -n <number> [options]

Advanced information gathering tool for phone numbers
(https://github.com/sundowndev/PhoneInfoga) version v1.6.8

optional arguments:
  -h, --help            show this help message and exit
  -n number, --number number
                        The phone number to scan (E164 or international
                        format)
  -i input_file, --input input_file
                        Phone number list to scan (one per line)
  -o output_file, --output output_file
                        Output to save scan results
  -s scanner, --scanner scanner
                        The scanner to use
  --recon               Launch custom format reconnaissance
  --no-ansi             Disable colored output
  -v, --version         Show tool version
```

```
➜  karma git:(master) ✗ python3 bin/karma.py search 123456789 --password --output result
> Starting

        X K U 9 0 S 5 S L
        7 0 K A R M A N L
        P H S P 6 I Q 0 I

        decoxviii
        15.03.19

> Searching
> Request password: 123456789
> Analyzing response
> Results:

+-----------------------------------------+-----------+
|                  Email                  | Password  |
+=========================================+===========+
| [redacted]-02-03-04-05@163.com          | 123456789 |
| [redacted]@bk.ru                        | 123456789 |
| [redacted]@gmail.com                    | 123456789 |
| [redacted]@hotmail.com                  | 123456789 |
| [redacted]@inbox.ru                     | 123456789 |
| [redacted]@list.ru                      | 123456789 |
| [redacted]@mail.ru                      | 123456789 |
| [redacted]@rambler.ru                   | 123456789 |
| [redacted]@yahoo.co.uk                  | 123456789 |
```

```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                     Version: 7.7.1
                   Codename: 'Blackout'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
```

vaultsecurity/osint

- The Harvester: **E-mails, subdomains and names Harvester - OSINT**
- Whois: **Get whois data**
- osrframework: **Open Sources Research Framework**
- R3dOv3r: **Know the dangers of credential reuse attacks**
- Buster: **Find emails of a person and return info associated with them**
- InstagramOsint: **An Instagram Open Source Intelligence Tool**
- Datasploit: **A tool to perform various OSINT techniques**
- Cloudfail: **Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network**
- WAFW00F: **WAFW00F identifies and fingerprints Web Application Firewall (WAF) products**

```
root@kali:~# theharvester

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: start in result number X (default: 0)
       -v: verify host name via dns resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```

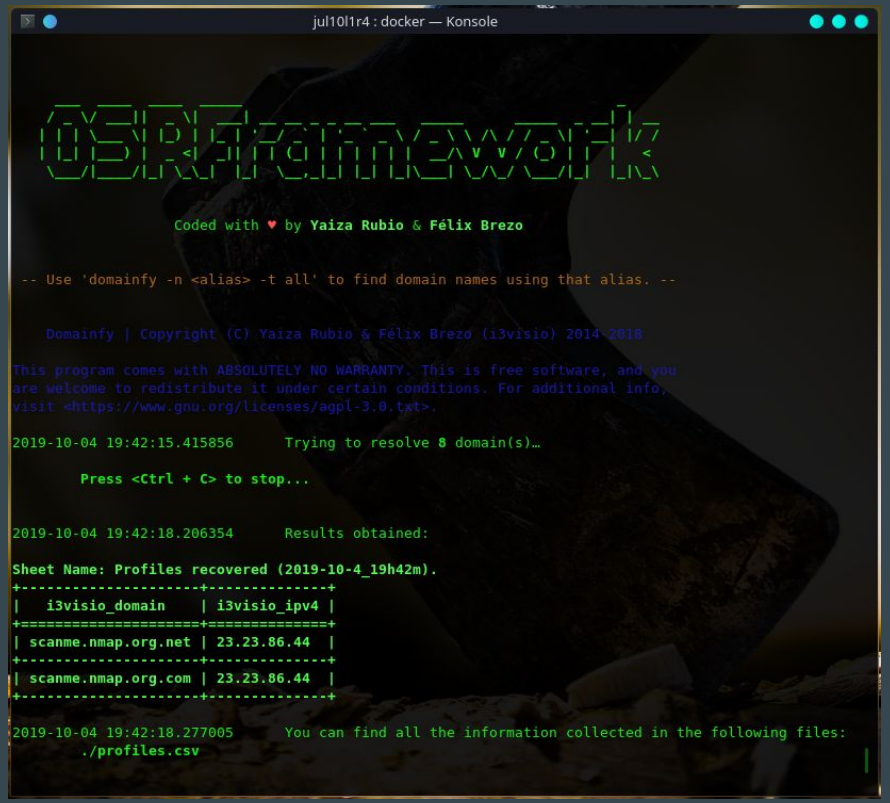
Open Sources Research Framework (OSRFramework)

domainfy -n 'scanme.nmap.org'

mailfy.py -n ‘i3visio’

searchfy.py -q "i3visio"

usufy.py -n i3visio -p twitter facebook



```
CREDOVER

Cr3d0v3r By D4Vinci - V0.4
  Know the dangers of email credentials reuse attacks.
     Loaded 14 website.

[+] Checking email in public leaks...
[+] Haveibeenpwned website results: 1
[+] Name : 000webhost | Date : 2015-10-26T23:35:45Z | What leaked : Email addresses,IP addresses,Names,Passwords
[+] Plaintext passwords found!
 │  └──── Sup3rPa$$w0rd357
 │
 └──=>Enter a password—=>

[+] Testing email against 14 website
[!] [ Facebook ] Login unsuccessful!
[!] [ Twitter  ] Login unsuccessful!
[!] [ Ask.fm   ] Login unsuccessful!
[!] [ Github   ] Login unsuccessful!
[!] [Virustotal] Login unsuccessful!
[!] [ Ebay.com ] Login unsuccessful!
[!] [Wikipedia ] Login unsuccessful!
[!] [ Airdroid ] Login unsuccessful!
[!] [ StackOF  ] Login unsuccessful!
[!] [FourSquare] Login unsuccessful!
[!] [ Gitlab   ] Login unsuccessful!
[+] [ Google   ] Login successful!
[!] [ Yahoo    ] Email not registered!
[!] [Mediafire ] Login unsuccessful!
```

```
root@ak:~# buster -e j*********4@y****.com -f john -l wyhko -b ****1974
[=]Validating 52 possible emails
[+]johnwyh1974@yahoo.com
        [-]Profiles:
                twitter
                facebook
        [-]Google Search:
                https://www.miribiz.com/directory/timber_industries
                http://miribiz33.rssing.com/chan-28092723/latest.php
                https://pastebin.com/dcipzPKz
                https://pastebin.com/6n8GF9N7
        [-]Breaches:
                Exactis
                LinkedIn
                OnlinerSpambot
        [-]Pastes:
                https://pastebin.com/GSYrPC35
                https://pastebin.com/pHZNPYK9
                https://pastebin.com/wz4JN5WK
                https://pastebin.com/sGRjX9Sc
                https://pastebin.com/zvfr4j0i
                https://pastebin.com/6n8GF9N7
```

```
bash-5.0# python3 main.py --username jairmessiasbolsonaro
```

INSTAGRAM OSINT

```
[*] Starting Scan on jairmessiasbolsonaro
Saved data to directory /workspace/InstagramOSINT/jairmessiasbolsonaro
--------------------------------------------
Results: scan for jairmessiasbolsonaro on instagram
Username:jairmessiasbolsonaro
Profile name:Jair M. Bolsonaro
URL:https://www.instagram.com/jairmessiasbolsonaro/
Followers:13.2m
Following:452
Posts:2,729
Bio:Capitão Paraquedista do Exército Brasileiro, eleito 38° Presidente da República Federativa do Brasil. 🇧🇷
profile_pic_url:https://instagram.fnat11-1.fna.fbcdn.net/vp/9a1c1ed735f7ef1ca6d7efc64c4147b3/5DE53B84/t51.2885-19/s320x320/44660219_1423978121070460_
2379675094759768064_n.jpg?_nc_ht=instagram.fnat11-1.fna.fbcdn.net
is_business_account:True
connected_to_fb:None
externalurl:https://youtu.be/aXDzRC3WR04
joined_recently:False
business_category_name:Creators & Celebrities
is_private:False
is_verified:True
```

```
root@localhost:~/Desktop/CloudFail# python cloudfail.py --target seo.com --tor

   ____ _                 _ _____       _ _
  / ___| | ___  _   _  __| |  ___|_ _(_) |
 | |   | |/ _ \| | | |/ _` | |_ / _` | | |
 | |___| | (_) | |_| | (_| |  _| (_| | | |
  \____|_|\___/ \__,_|\__,_|_|  \__,_|_|_|
    v1.0                          by m0rtem


[16:37:54] Initializing CloudFail - the date/time is: 12/06/2016 16:37:54
[16:38:00] TOR connection established!
[16:38:00] New IP: 5.135.158.101
[16:38:00] Fetching initial information from: seo.com...
[16:38:00] Server IP: 104.28.2.64
[16:38:00] Testing if seo.com is on the Cloudflare network...
[16:38:00] seo.com is part of the Cloudflare network!
[16:38:00] Testing for misconfigured DNS using dnsdumpster...
[16:38:03] [FOUND:HOST] toolsapi.seo.com  107.170.121.228 AS62567 Digital Ocean, Inc. Ur
[16:38:03] [FOUND:HOST] cm.seo.com Apache/2.4.7 (Ubuntu) 198.199.116.160 AS14061 Digital
[16:38:03] [FOUND:HOST] crm.seo.com nginx/1.4.6 (Ubuntu) 192.241.202.147 AS14061 Digital
[16:38:03] [FOUND:HOST] deathstar.seo.com Apache/2.4.6 (CentOS) PHP/5.4.16 104.236.144.1
[16:38:03] [FOUND:HOST] deathdev.seo.com  209.90.66.178 AS5048 FIBERNET Corp. United Sta
[16:38:03] [FOUND:HOST] host.seo.com nginx 173.255.232.177 AS8001 Net Access Corporatior
[16:38:03] [FOUND:MX] 64.233.190.26 AS15169 Google Inc. 30 alt2.aspmx.l.google.com.
[16:38:03] [FOUND:MX] 74.125.141.26 AS15169 Google Inc. 20 alt1.aspmx.l.google.com.
[16:38:03] [FOUND:MX] 74.125.141.26 AS15169 Google Inc. 40 aspmx2.googlemail.com.
[16:38:03] [FOUND:MX] 64.233.176.26 AS15169 Google Inc. 10 aspmx.l.google.com.
[16:38:03] [FOUND:MX] 64.233.190.26 AS15169 Google Inc. 50 aspmx3.googlemail.com.
[16:38:03] Scanning crimeflare database...
[16:38:05] [FOUND:IP] 173.255.232.177
[16:38:05] [FOUND:IP] 198.74.56.156
[16:38:05] [FOUND:IP] 209.90.89.217
[16:38:05] Scanning 2898 subdomains, please wait...
[16:38:34] [FOUND:SUBDOMAIN] FOUND: blog.seo.com IP: 173.255.232.177 HTTP: 200
[16:38:38] [FOUND:SUBDOMAIN] FOUND: blogs.seo.com IP: 173.255.232.177 HTTP: 200
[16:39:04] [FOUND:SUBDOMAIN] FOUND: client.seo.com IP: 173.255.232.177 HTTP: 200
```

```
                 _______
                /       \
               (  Woof! )
                \_______/                          )
                ,,                               ) (_
          .-. -     ________                    ( |__|
         ()``; |==|________)                    .)|__|
         / ('        /|\                       (  |__|
      (  /  )       / | \                       . |__|
       \(_)_))     /  |  \                        |__|
```

WAFW00F - Web Application Firewall Detection Tool

Vault-Cyber-Security/osint

Repo: github.com/Vault-Cyber-Security/osint

./install-osint.sh

```
19  _install_pip(){
20    run="$1 install $2 --user"
21    echo -e "Run: $orange$run$end"
22    eval "$run" && echo -e "$correct Installed(s): $2" || echo -e "$incorrect Error in install of: $2"
23  }
24
25  _install_git(){
26    cd "/workspace"
27    run="git clone $1"
28    echo -e "Run: $orange$run$end"
29    eval "$run" && echo -e "$correct Installed(s): $1" || echo -e "$incorrect Error in install of: $1"
30    cd "$here"
31  }
32  _run(){
33    echo -e "Run: $orange$1$end"
34    eval "$1" && echo -e "$correct $1" || echo -e "$incorrect $1"
35  }
```

Docker

Repo: hub.docker.com

==========

docker run -it vaultsecurity/osint:beta bash

Comunidade de OSINT

Grupo: @osint_br

Canal: @osint_channel

Julio Lira (Jujublau)

Telegram: @juraul

Email: jul10l1r4@disroot.org

Github: @jul10l1r4

Notabug: @jul10l1r4